Cuidado con el “bluesnarfing”: el nuevo método que roba datos vía bluetooth

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno emitió una advertencia para aquellas personas con dispositivos con bluetooth. Esto, por el riesgo que supone su uso, ya que los ciberdelincuentes pueden robar datos e incluso suplantar la identidad.

El académico de la Facultad de Ingeniería y Ciencias Aplicadas de la Universidad de los Andes, Claudio Álvarez, explica que lo que ocurre es “que el delincuente toma control de un dispositivo, víctima a través de bluetooth, y esto normalmente se debe a alguna falencia del sistema operativo Android o IOS”, comenta.

También hay bluesnarfing, en términos de que el delincuente puede sustraer información personal información financiera y con eso realizar suplantación de identidad, fraudes en comercios y cuestiones por el estilo.

Entonces, comenta Álvarez, este método “afecta a cualquier usuario que pueda tener dispotivo móvil con bluetooth y que lo mantenga encendido, sobre todo en lugares públicos de alta concurrencia, porque es ahí donde más ocurren los ataques de bluesnarfing. En cualquier evento público, también, los ciberdelincuentes pueden estar escaneando el ambiente, para poder encontrar dispositivos que puedan ser explotables”, menciona.

¿Cómo evitar el bluesnarfing?

- Mantener el bluetooth apagado si no se están usando audífonos inalámbricos o el teléfono en el auto.
- Mantener el sistema operativo a su última versión.
- Descargar inmediatamente las actualizaciones del fabricante cuando aparece.
- Evitar conexiones con dispositivos desconocidos.

Cuidado con el “bluesnarfing”: el nuevo método que roba datos vía bluetooth

y tú, ¿qué opinas?